UNCLASSIFIED

3 August 2015

NORTH DAKOTA

HOMELAND SECURITY

Cyber Summary

North Dakota State and Local Intelligence Center

NDSLIC

1-866-885-8295

The North Dakota Open Source Cyber Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Cyber Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC Disclaimer

The Cyber Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

Table of Contents

North Dakota

Nothing Significant to Report

Regional

Nothing Significant to Report

National

(National) FireEye: Kremlin-backed hackers used Twitter to mask attacks on U.S. FireEye the other day released a new Threat Intelligence report which analyzes the functionality and obfuscation tactics of an advanced piece of malware employed by the likely Russian government-backed Advanced Persistent Threat (APT) group APT29. APT29 combines steganography, cloud storage, and social media services to fly under the radar of network defenders. http://www.homelandsecuritynewswire.com/dr20150731-fireeye-kremlinbacked-hackers-used-twitter-to-mask-attacks-on-u-s\

International

(International) Russia offers safe haven for a major botnet operator. Recently the FBI offered a reward of $3 million for any useful information which will lead to the apprehension of Evgeniy Mikhailovich Bogachev. Bogachev is notorious for creating the Gameover Zeus botnet, which the FBI had successfully shut down in mid-2014, but the agency failed to capture Bogachev himself. In early 2015 Bogachev managed to restore Zeus.The hackers behind Zeus are believed to have stolen more than $100 million since3 2011. Experts worry that botnet may be used for more than stealing money, and may become a weapon of cyber warfare. Bogachev and some members of his hacking crew now live in Russia, and the Russian government does not want to hand him or any of his hackers over to the United States to stand trial. http://www.homelandsecuritynewswire.com/dr20150727-russia-offers-safe-haven-for-a-major-botnet-operator

(International) Russian hacker tool uses legitimate Web services to hide attacks: FireEye. Security researchers from FireEye discovered that the APT29 threat group is employing a malicious backdoor dubbed "HAMMERTOSS" that utilizes a multi-stage process involving social media, steganography, and PowerShell to

hide malicious activity within legitimate network traffic. Researchers believe that the backdoor is only being deployed against critical targets, possibly as a backup in case other tools fail or are disrupted.
http://www.securityweek.com/russian-hacker-tool-uses-legitimate-web-services-hide-attacks-fireeye

(International) More than a third of employees would sell company data. Loudhouse released results from a survey on enterprise security practices polling over 500 Internet technology (IT) decision-makers and 4,000 employees across the U.S., Europe, and Australia, revealing that 25 percent of employees polled would sell company data for less than $8,000, citing the ready access most employees have access to valuable data, among other findings.
http://www.net-security.org/secworld.php?id=18682

(International) **Data breach may help Chinese government identify U.S. spies.** Several American government and intelligence officials have expressed concerns that this summer's sweeping data breach of the United States Office of Personnel Management may have further ramifications. According to reporting by The New York Times, officials believe that combined with China's prior accumulated data and intelligence, data troves from the OPM hack could give the Chinese government the information necessary to hone in on the identities of American spies.
http://www.pbs.org/newshour/rundown/data-breach-might-help-chinese-government-identify-u-s-spies/

Banking and Finance Industry

(National) How vulnerable are the U.S. stock markets to hackers? An analysis of information security and cyber risk trends in the financial sector cited findings from a 2015 U.S. Securities and Exchange Commission Risk Alert revealing that about 88 percent of brokerages and 74 percent of financial advisers in the U.S. have suffered cyber-attacks, and that according to Congressional testimony, a major U.S. bank is attacked every 34 seconds, among other disclosures.
http://www.marketwatch.com/story/how-vulnerable-are-the-us-stock-markets-to-hackers-2015-07-31

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(International) Honeywell Patches Flaws in Tuxedo Touch Home Automation Controller. Last week , a discovery was made that the Tuxedo Touch controller is plagued by flaws that can be exploited by an attacker to bypass authentication mechanisms and access restricted pages, and trick legitimate users into issuing various commands. The security bugs have been patched by Honeywell with the release of firmware version TUXW_V5.2.19.0_VA, which can be downloaded by clicking this link.
http://www.securityweek.com/honeywell-patches-flaws-tuxedo-touch-home-automation-controller

Communications Sector

(International) Android Stagefright flaws put 950 million devices at risk. Security researchers at Zimperium zLabs reported that about 950 million Android devices are vulnerable to flaws in the operating system's (OS) Stagefright media engine, in which excessive permissions could allow an attacker to send a Multimedia Messaging Service (MMS) or Google Hangouts message to trigger the vulnerability, granting system access on the affected device.
https://threatpost.com/android-stagefright-flaws-put-950-million-devices-at-risk/113960

(International) Over 5,000 mobile apps found performing in-app ad fraud. Security researchers from Forensiq discovered at least 5,000 mobile applications being used for mobile hijacking ad fraud worldwide that were observed affecting 12 million unique devices over a 10-day period.
http://www.net-security.org/secworld.php?id=18667

(International) Apple App Store and iTunes buyers hit by zero-day. Security researchers from Vulnerability Lab published a zero-day filter bypass flaw in Apple's online invoicing system used in its App Store and iTunes that could allow an attacker to hijack a user's purchasing session to buy and download any app or content they want, before charging it to the original user.

http://www.scmagazineuk.com/apple-app-store-and-itunes-buyers-hit-by-zero-day/article/428864/

Critical Manufacturing

(National) GM quickly issues fix for OnStar hack, but service still vulnerable. The General Motors Company confirmed July 30 that OnStar-equipped vehicles are vulnerable to a flaw that could allow an attacker to remotely locate the vehicle and issue commands through OnStar's RemoteLink app, such as locking doors or starting the engine. A hacker demonstrated the vulnerability using a device called "OwnStar," which he claimed allowed him to intercept communications between the app and the vehicle.
http://www.cnet.com/news/ownstar-onstar-hack/

(California) Two charged in 2011 cyber breach at Michaels retailer. Two California residents were indicted July 30 on charges alleging that they were conspirators to a 2011 cyberattack in which 94,000 credit and debit card numbers were stolen from Michaels Stores Inc., customers.
http://www.businessinsurance.com/article/20150731/NEWS06/150739970/two-charged-in-2011-cyber-breach-at-michaels-retailer?tags

Defense/ Industry Base Sector

(National) U.S. military bases vulnerable to cyberattacks on their power, utility systems. U.S. military bases are at risk for cyberattacks against the bases' power grid and other utility systems, according to a new report on defense infrastructure from the Government Accounting Office.
http://www.homelandsecuritynewswire.com/dr20150730-u-s-military-bases-vulnerable-to-cyberattacks-on-their-power-utility-systems

Emergency Services

Nothing Significant to Report

Energy

Nothing Significant to Report

Food and Agriculture

Nothing Significant to Report

Government Sector (including Schools and Universities)

(National) GAO: defense installation utilities at risk of cyber attack. A recent report released by the U.S. Government Accountability Office warned against vulnerabilities in the military's industrial control systems (ICS) network controlling essential services to military installations worldwide. A 2018 deadline set by the Pentagon to address limited cyber defenses for the ICS will be difficult to meet due to delays and unreliable data, according to the report.
http://www.militarytimes.com/story/military/2015/07/24/utility-cyber-attack/30615033/

Information Technology and Telecommunications

(International) Hacking Forum Darkode Resurfaces. The Darkode cybercrime forum will return online soon. The news comes less than two weeks after law enforcement authorities announced that they had brought down the website. The forum will be relaunched soon and its administrators are implementing new security measures to protect the website and its members.
http://www.securityweek.com/hacking-forum-darkode-resurfaces

(International) Cybercriminals use Angler exploit kit to target PoS systems. Trend Micro researchers reported that cybercriminals have been utilizing the Angler exploit kit (EK) to deliver a reconnaissance trojan that detects mitigation tools before downloading one of three point-of-sale (PoS) malware payloads.
http://www.securityweek.com/cybercriminals-use-angler-exploit-kit-target-pos-systems

(International) Over 10 million Web surfers possibly exposed to malvertising. Cyphort released tracking data from malicious advertisement campaigns revealing that since July 18, over 10 million people may have visited Web sites containing malicious ads which redirect visitors to directories hosting the Angler exploit kit (EK).
http://www.computerworld.com/article/2953256/security/over-10-million-web-surfers-possibly-exposed-to-malvertising.html#tk.rss_security

(International) Software vulnerabilities hit a record high in 2014, report says. Secunia released analysis from its Vulnerability Review 2015 revealing that the number of recorded software vulnerabilities hit a record high of 15,435 in 2014, an increase of 18 percent from the previous year, and that many organizations are too slow to release security fixes, among other findings.
http://www.networkworld.com/article/2953304/security/software-vulnerabilities-on-the-rise-record-high-report.html#tk.rss_all

(International) Phishing attacks drive spike in DNS threat. Infoblox and Internet Identity published data revealing that the Domain Name System (DNS) Threat Index jumped nearly 60 percent in the second quarter of 2015, reportedly due to a corresponding 74 percent increase in phishing and phishing domains over the same period.
http://www.darkreading.com/attacks-breaches/phishing-attacks-drive-spike-in-dns-threat/d/d-id/1321480

(International) CyberX Launches Industrial Threat Intelligence Initiative. Industrial cybersecurity startup CyberX has launched its Industrial Threat Intelligence Platform, which the company says can help utilities identify cyber security threats in operational networks.
http://www.securityweek.com/cyberx-launches-industrial-threat-intelligence-initiative

(International) Row Hammer DRAM bug now exploitable via JavaScript, most DDR3 memory chips vulnerable. Security researchers from universities in Austria and France released findings revealing that the Row Hammer exploit can be initiated and actively exploited remotely via JavaScript, making it the first documented "remote software-induced hardware-fault attack."
http://news.softpedia.com/news/row-hammer-dram-bug-now-exploitable-via-javascript-488050.shtml

(International) Google fixes Chrome issue that leaked the user's real IP from behind a VPN. Google released a Chrome Web browser extension called "WebRTC Network Limiter" to address an issue with the WebRTC protocol in which certain circumstances could reveal the real public and local Internet Protocol (IP) address of a user connected via a virtual private network (VPN).

http://news.softpedia.com/news/google-fixes-chrome-issue-that-leaked-the-user-s-real-ip-from-behind-a-vpn-488143.shtml

US-Cert Updates and Vulnerabilities

(International) BIOS implementations fail to properly set UEFI write protections after waking from sleep mode. Multiple BIOS implementations fail to properly set write protections after waking from sleep, leading to the possibility of an arbitrary BIOS image reflash. A privileged attacker with console access can reflash the BIOS of affected systems to an arbitrary image. The current solution is to apply an update. Refer to the Vendor Information section below for a list of affected Dell products, and visit their support page to download updates. Apple updates addressing this issue have been pushed via the App Store beginning June 30, 2015. We are continuing to communicate with vendors as they investigate this vulnerability.
http://www.kb.cert.org/vuls/id/577140

(International) Cisco Releases Security Updates. Cisco has released software updates to address a vulnerability in Cisco IOS XE Software for ASR 1000 Series Aggregation Services Routers. Exploitation of this vulnerability may allow a remote attacker to cause a denial-of-service condition.
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150730-asr1k

(International) Chiyu Technology fingerprint access control contains multiple vulnerabilities. Multiple models of Chiyu Technology fingerprint access control devices contain a cross-site scripting (XSS) vulnerability and an authentication bypass vulnerability. The CERT/CC is currently unaware of a practical solution to this problem.
http://www.kb.cert.org/vuls/id/360431

ICS-Cert Alerts & Advisories

(International) Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 Password Storage Vulnerability. Gleb Gritsai, Alisa Esage Shevchenko, Ilya Karpov, and the team from Positive Technologies Security have found sensitive information stored in clear text in the Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 products. Schneider Electric has released new patches to mitigate this vulnerability.
https://ics-cert.us-cert.gov/advisories/ICSA-15-211-01

Public Health

(International) Many high-profile firms using vulnerable PHP File Manager: researcher. A security researcher identified several vulnerabilities in Revived Wire Media's PHP File Manager application, including the existence of a default user account with backdoor access to systems running the software, lack of protection for the user database, and arbitrary file upload vulnerabilities, among other flaws. Many firms reportedly still use the application even though it has not been updated since its release in 2010 – 2011.
http://www.securityweek.com/many-high-profile-firms-using-vulnerable-php-file-manager-researcher

(Georgia) Patient information released in Georgia agency data breach. The Georgia Department of Human Services Division of Aging Services notified approximately 3,000 people served by the agency's Community Care Services Program of a data breach involving health diagnoses through an email to a contracted provider July 28.
http://www.bizjournals.com/atlanta/morning_call/2015/07/patient-information-released-in-state-agency-data.html

(New York) Healthfirst: 5,300 members exposed in fraud incident. Healthfirst, which provides care to over one million members in New York, announced July 24 that nearly 5,300 of its current members had personal information compromised after a hacker gained access to the company's online portal April 11, 2012 – March 26, 2014. A suspect has been identified and charged with fraud, and those affected will be provided free identity theft, credit monitoring, and credit restoration services for one year.
http://www.securityweek.com/healthfirst-5300-members-exposed-fraud-incident

(Ohio) Patient data included on missing thumb drive, OhioHealth says. OhioHealth Riverside Methodist Hospital announced July 24 the potential breach of sensitive data for 1,006 valve-replacement candidates and research subjects after an unencrypted flash drive was found missing May 29. Hospital officials do not believe the flash drive was stolen or used inappropriately, and OhioHealth is transitioning to encrypted flash drives in hospitals throughout the State.
http://www.dispatch.com/content/stories/local/2015/07/27/OhioHealth-thumb-drive-missing.html

Transportation

(International) United Airlines Hack Highlights Need for Improved Information Sharing. The same cyber-attackers who breached the Office of Personnel Management and healthcare giant Anthem appear to have also stolen flight manifests containing passenger information from United Airlines earlier this year, according to reports.
http://www.securityweek.com/united-airlines-hack-highlights-need-improved-information-sharing\

(International) China-tied hackers that hit U.S. said to breach United Airlines. Investigators involved in a probe of a previously unreported May or June breach of United Airlines' computer systems reported links between the hackers and the Chinese threat group that perpetrated the theft of security-clearance records from the U.S. Office of Personnel Management and medical data from Anthem Inc., as well as at least seven other travel and health insurance organizations. Officials believe that the breach may have compromised movement data of millions of Americans and opened the airline's systems to future disruptions and attacks.
http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines

Water and Dams

Nothing Significant to Report

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165